This Page Is Inserted by IFW Operations
and is not a part of the Official Record

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images may include (but are not limited to):

- BLACK BORDERS
- TEXT CUT OFF AT TOP, BOTTOM OR SIDES
- FADED TEXT
- ILLEGIBLE TEXT
- SKEWED/SLANTED IMAGES
- COLORED PHOTOS
- BLACK OR VERY BLACK AND WHITE DARK PHOTOS
- GRAY SCALE DOCUMENTS

IMAGES ARE BEST AVAILABLE COPY.

As rescanning documents *will not* correct images, please do not report the images to the Image Problems Mailbox.

This Page Blank (uspto)

(19) RÉPUBLIQUE FRANÇAISE

INSTITUT NATIONAL
DE LA PROPRIÉTÉ INDUSTRIELLE

PARIS

(11) **N° de publication :** **2 757 661**
(à n'utiliser que pour les commandes de reproduction)

(21) **N° d'enregistrement national :** **96 15980**

(51) Int Cl[6] : **G 06 K 19/073**, G 06 K 5/00, G 07 F 7/08, H 04 L 9/32, 12/28, G 06 F 17/60 //G 06 F 157:00, 151:00

(12) DEMANDE DE BREVET D'INVENTION A1

(22) **Date de dépôt** : 24.12.96.

(30) **Priorité** :

(43) **Date de la mise à disposition du public de la demande :** 26.06.98 Bulletin 98/26.

(56) **Liste des documents cités dans le rapport de recherche préliminaire :** *Se reporter à la fin du présent fascicule.*

(60) **Références à d'autres documents nationaux apparentés :**

(71) **Demandeur(s) :** *GEMPLUS SOCIETE EN COMMANDITE PAR ACTIONS* — FR.

(72) **Inventeur(s) :** VANNEL PIERRE.

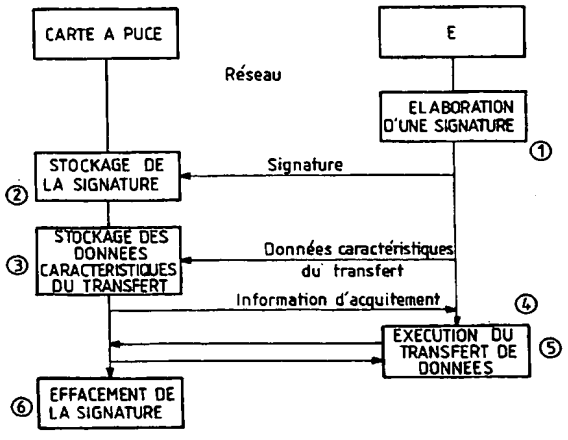
(73) **Titulaire(s) :** .

(74) **Mandataire :** CABINET BALLOT SCHMIT.

(54) PROCEDE DE TRANSFERT SECURISE DE DONNEES PAR UN RESEAU DE COMMUNICATION.

(57) L'invention concerne les transferts de données réalisés par un réseau de communications. Elle concerne notamment un procédé de transfert sécurisé de données par un réseau de communications, entre une première entité constituée par une carte à puce et une deuxième entité, selon lequel on élabore au préalable une signature électronique, permettant de prouver l'initialisation du transfert, cette signature étant stockée dans au moins une zone mémoire de la carte à puce puis, lorsque le transfert de données est terminé, on efface cette signature.

Application au porte-monnaie électronique.



FR 2 757 661 - A1

BNSDOCID: <FR 2757661A1>

PROCÉDÉ DE TRANSFERT SÉCURISÉ DE DONNÉES PAR UN RÉSEAU DE COMMUNICATION

L'invention concerne les transferts de données réalisés par un réseau de communications. Ce réseau peut par exemple être le réseau téléphonique commuté, le réseau de communication cellulaire tel que le réseau au standard Européen G.S.M ou encore le réseau INTERNET.

Dans le cas des échanges classiques de données entre deux entités, l'authenticité de ces données échangées est garantie par une signature électronique. Cette signature électronique peut être obtenue à l'aide de mécanismes de cryptographie divers tels que des mécanismes de chiffrement, ou d'authentification, ou de signature au sens propre. L'algorithme de calcul correspondant peut être symétrique, auquel cas la clé secrète de signature est partagée par les deux entités, ou asymétrique, auquel cas la clé secrète de signature n'est connue que de l'entité signataire. De tels procédés de transfert de données, permettant l'authentification des données échangées, sont notamment décrits dans la demande de brevet EP - A - 0 683 582 et dans la demande de brevet US 5,534,683.

Aujourd'hui, nous assistons à un fort développement des applications grand public sur des réseaux de communications susceptibles de permettre l'utilisation de cartes à puce. Cependant , l'opération de transfert de données par un réseau est délicate à mettre en oeuvre puisqu'elle peut comporter des échanges entre plusieurs entités et une carte à puce. Les échanges de données par l'intermédiaire d'un réseau peuvent en outre être interrompus pour de multiples raisons telles que, par exemple, la rupture d'une communication,

BNSDOCID: <FR 2757661A1>

l'arrachement de la carte à puce ou une panne de l'entité échangeant des données avec la carte à puce. Cette interruption entraîne une désynchronisation des deux entités au détriment de l'une d'entre elles. Les mécanismes connus à ce jour ne permettent pas d'éviter ce problème de désynchronisation en cas d'interruption au cours d'un transfert de données.

La présente invention permet de résoudre ce problème de désynchronisation de deux entités susceptibles d'apparaître lors d'une interruption et propose un procédé de transfert sécurisé de données par un réseau de communications, entre une première entité constituée par une carte à puce et une deuxième entité, apte à garantir l'usage de la carte à puce dans toutes les circonstances même dans le cas d'interruptions au cours de transactions. Ce procédé consiste à élaborer au préalable une signature électronique, permettant de prouver l'initialisation du transfert, et à la stocker dans au moins une zone mémoire de la carte à puce puis, lorsque le transfert est terminé, à effacer cette signature.

Selon une autre caractéristique de l'invention, le procédé comporte une procédure de réclamation, cette procédure consistant à vérifier la présence ou l'absence de la signature dans une zone mémoire de la carte à puce, afin de savoir si le transfert de données a échoué ou abouti.

Selon une autre caractéristique de l'invention, lorsque le transfert de données a été interrompu, la procédure de réclamation consiste en outre à:

- élaborer une nouvelle signature électronique,
- remplacer la signature du transfert échoué par ladite nouvelle signature,

BNSDOCID: <FR 2757661A1>

- effectuer les étapes du transfert non encore exécutées, puis

- effacer la nouvelle signature lorsque le transfert est terminé.

Selon une autre caractéristique de l'invention, la signature est stockée de manière sécurisée dans une zone mémoire afin qu'elle ne soit accessible par l'extérieur ni en lecture ni en écriture.

De manière avantageuse, cette zone mémoire est une zone de mémoire électriquement programmable de type EEPROM.

Selon une autre caractéristique de l'invention la signature est élaborée par la deuxième entité et effacée par l'électronique la carte à puce.

Selon une autre caractéristique de l'invention, la signature peut être élaborée au moyen d'un algorithme de cryptographie.

Selon une autre caractéristique de l'invention les données transférées sont des unités de valeur. Dans ce cas la carte à puce peut être un porte-monnaie électronique.

Selon une autre caractéristique de l'invention, le procédé de transfert de données peut être appliqué à une transaction financière entre un organisme bancaire et un porte-monnaie électronique pour créditer le contenu du porte-monnaie, ou entre un fournisseur de services et un porte-monnaie électronique pour débiter le contenu du porte-monnaie.

Selon une autre caractéristique de l'invention, le procédé de transfert de données peut être appliqué à une transaction d'unités de valeurs entre un organisme de jeux et une carte à puce.

La présente invention permet d'éviter des déséquilibres éventuels, susceptibles de se créer entre

BNSDOCID: <FR 2757661A1>

deux entités, causés par des interruptions au cours de transferts de données. En effet, la présence de la signature électronique dans une zone mémoire de la carte à puce, après une opération de transfert, indique l'existence d'un déséquilibre et constitue la preuve que l'opération a échoué. Le rétablissement de l'équilibre dans les échanges est réalisé à l'initiative de l'utilisateur de la carte à puce. D'autre part une signature électronique correspondant à un transfert n'est utilisable qu'une seule fois.

D'autres particularités et avantages de l'invention apparaîtront à la lecture de la description faite à titre d'exemple non limitatif en référence aux figures annexées qui représentent:

- la figure 1, un schéma de principe d'un dispositif de mise en oeuvre d'un procédé selon l'invention,
- la figure 2, un organigramme d'un procédé de transfert de données selon l'invention,
- la figure 3, un organigramme d'une procédure de réclamation permettant d'exécuter les étapes du procédé de transfert qui ont été interrompues,
- la figure 4A, un organigramme d'un procédé de transfert appliqué à une transaction financière, entre un organisme bancaire et un porte-monnaie électronique,
- la figure 4B, un organigramme d'une procédure de réclamation permettant l'exécution d'étapes ayant été interrompues au cours de la transaction de la figure 4A,
- la figure 5A, un organigramme d'un procédé de transfert appliqué à une transaction financière entre un porte-monnaie électronique et un fournisseur de services,

BNSDOCID: <FR 2757661A1>

- la figure 5B, un organigramme d'une procédure de réclamation permettant l'exécution d'étapes ayant été interrompues au cours de la transaction de la figure 5A.

Le procédé de transfert de données selon l'invention est réalisé entre deux entités dont l'une est de préférence une carte à puce.

La carte à puce utilisée comprend de façon connue un microprocesseur relié par un bus aux différentes mémoires et aux ports d'entrée/sortie de la carte. Parmi les mémoires, il y a en général:

- une mémoire volatile de travail RAM, comme il y en a dans tous les systèmes à microprocesseurs, pour stocker les données intermédiaires nécessaires au cours d'une utilisation de la carte,

- une mémoire morte ROM, contenant des programmes de système permettant le fonctionnement de la carte, programmes qui ne varient pas d'une utilisation à une autre de la carte;

- une mémoire effaçable et programmable électriquement EEPROM, pour l'enregistrement de données destinées à être modifiées et mises à jour au cours des utilisations successives de la carte.

La figure 1 illustre un schéma de principe d'un dispositif de mise en oeuvre d'un procédé de transfert de données selon l'invention. Une carte à puce C est introduite dans la fente d'un organe lecteur enregistreur dénommé dans la suite lecteur L qui peut par exemple être un ordinateur. Le lecteur L est relié, par l'intermédiaire d'un réseau R, à plusieurs entités E1, E2, ...EN susceptibles d'échanger des données avec la carte à puce C.

BNSDOCID: <FR 2757661A1>

L'organigramme de la figure 2 illustre les différentes étapes d'un procédé de transfert de données selon l'invention, entre une première entité telle qu'une carte à puce et une deuxième entité E, par l'intermédiaire d'un réseau. Dans une première étape 1, l'entité E élabore une signature électronique pour indiquer l'initialisation du transfert. L'entité commande alors l'écriture de cette signature dans au moins une zone mémoire de la carte à puce, c'est l'étape 2. Cette signature électronique est enregistrée sécuritairement dans cette zone mémoire, c'est-à-dire qu'elle est stockée de manière à ce qu'elle ne soit accessible ni en lecture ni en écriture par l'extérieur. De préférence, la zone mémoire dans laquelle elle est stockée est une zone de mémoire électriquement programmable de type EEPROM.

L'entité E peut en outre posséder des algorithmes de cryptographie de manière à assurer la confidentialité de la signature.

Les étapes suivantes 3, 4 et 5 consistent à effectuer le transfert de données. Pour cela, l'entité commande l'écriture, dans une autre zone de la mémoire EEPROM de la carte à puce, des données caractéristiques du transfert (étape 3). La carte à puce renvoie alors une information d'acquittement selon laquelle elle autorise le transfert (étape 4), puis le transfert est exécuté (étape 5). Lorsque le transfert de données est terminé, le microprocesseur de la carte à puce commande l'effacement de la signature stockée en mémoire (étape 6).

Si une interruption du transfert, due à une rupture de communication, un arrachement intempestif de la carte à puce ou une panne de l'entité E par exemple, se produit entre les étapes 4 et 5 un déséquilibre risque

BNSDOCID: <FR 2757661A1>

de se créer au détriment de l'une des deux entités. Grâce au procédé selon l'invention, un tel déséquilibre peut être mis en évidence par la présence de la signature qui n'aura pas été effacée de la mémoire de la carte à puce. La présence de cette signature indique donc une situation d'erreur possible. Le rétablissement de l'équilibre est alors effectué à l'initiative de l'utilisateur de la carte en réalisant une nouvelle connexion entre les deux entités par l'intermédiaire du réseau.

La carte à puce commande alors le déroulement d'une procédure de réclamation dont l'organigramme est représenté sur la figure 3.

Dans un premier temps, à l'étape 4a, l'entité E vérifie la présence ou l'absence de la signature dans la zone mémoire de la carte à puce qui lui est réservée, de manière à vérifier si le transfert de données a échoué ou abouti.

Dans le cas où la signature est présente, c'est à dire lorsque le transfert a échoué, l'entité E élabore alors une nouvelle signature électronique et commande le remplacement de la première signature correspondant au transfert échoué par cette nouvelle signature, c'est l'étape 4b.

Le procédé mis en oeuvre, pour mettre à jour cette signature de manière sécurisée, pourra être par exemple celui qui est décrit dans la demande de brevet FR 95 01791.

L'étape suivante 4c consiste à exécuter les étapes du transfert de données qui ont été interrompues. Enfin, lorsque le transfert de données a été entièrement et correctement exécuté, la nouvelle signature est effacée (étape 4e).

BNSDOCID: <FR 2757661A1>

Les données transférées peuvent notamment être des unités de valeurs.

De manière avantageuse, la carte à puce peut être réalisée sous forme de porte-monnaie électronique.

Une application particulière du procédé selon l'invention concerne une transaction financière entre un porte-monnaie électronique (carte C) et un organisme bancaire (entité E1) ou entre un porte-monnaie électronique et un organisme de fourniture de service (entité E2).

Dans ce cas, une unité de valeur correspond, de manière avantageuse, à une unité monétaire.

Une transaction entre un porte-monnaie et un organisme bancaire consiste plus particulièrement à créditer le contenu du porte-monnaie, tandis qu'une transaction entre ce porte-monnaie et un organisme de fourniture de service consiste à le débiter.

La gestion du stockage et de l'effacement de la signature dans la mémoire EEPROM du porte-monnaie électronique dépend du type d'opération effectuée. Elle est en effet différente selon que l'opération consiste à créditer ou à débiter le contenu du porte-monnaie électronique. Cette gestion est expliquée plus en détail dans ce qui suit.

L'organigramme de la figure 4A illustre le chargement d'un porte-monnaie électronique au cours d'une transaction financière avec un organisme bancaire.

Dans l'exemple représenté sur cette figure, préalablement à l'initialisation de la transaction, le contenu du porte-monnaie comporte 5 unités de valeur UV, et le compte bancaire de l'utilisateur du porte-monnaie comporte 500 UV.

BNSDOCID: <FR 2757661A1>

Lorsqu'un utilisateur demande le chargement de son porte-monnaie d'une valeur de 100 unités de valeurs UV par exemple (étape 10), la banque, après avoir vérifié le solde du compte utilisateur, construit une preuve de la transaction, c'est-à-dire qu'elle calcule une signature électronique, et la transmet au porte-monnaie (étape 20).

Le porte-monnaie stocke la signature électronique et les données caractéristiques de la transaction dans une zone de mémoire EEPROM et renvoie à la banque une information d'acquittement autorisant l'exécution de la transaction (étape 30).

La banque débite alors le compte utilisateur et ordonne le chargement correspondant du porte-monnaie (étape 40). Le crédit est effectué et, simultanément, le porte-monnaie efface la signature en mettant en oeuvre le procédé de mise à jour sécurisée de mémoire EEPROM décrit dans la demande de brevet FR 95 01791.

Lorsque l'opération de transaction est terminée, le contenu du porte-monnaie électronique doit par conséquent être égal à 105 UV, tandis que le contenu du compte bancaire de l'utilisateur du porte-monnaie est égal à 400 UV.

Une interruption entre les étapes 30 et 40 peut entraîner un déséquilibre entre le porte-monnaie et la banque au détriment de l'utilisateur. En effet, il se peut que le compte bancaire de l'utilisateur ait été débité alors que son porte-monnaie n'a pas été crédité.

Cependant, lorsqu'une telle interruption se produit, le chargement du porte-monnaie n'ayant pas abouti, la signature n'est pas effacée de la mémoire EEPROM du porte-monnaie. La présence de cette signature permet donc de prouver que la transaction a échoué. L'utilisateur doit alors reconnecter son porte-monnaie

BNSDOCID: <FR 2757661A1>

à l'organisme bancaire, par l'intermédiaire du réseau, pour rétablir l'équilibre.

Lors de la reconnexion, le microprocesseur du porte-monnaie électronique lance le déroulement d'une procédure de réclamation, dont l'organigramme est illustré sur la figure 4B.

Dans l'exemple de la figure 4B, le compte bancaire de l'utilisateur a été débité de 100 UV et est égal à 400 UV, alors que le contenu du porte monnaie n'a pas été crédité et est resté égal à 5 UV.

Lors de la réclamation, le porte-monnaie présente donc à la banque les données caractéristiques de la transaction et la preuve que cette transaction a été interrompue, c'est-à-dire la signature électronique (étape 31). La banque vérifie cette signature électronique et valide la procédure de réclamation. Puis elle construit une nouvelle preuve de la transaction et la transmet au porte-monnaie (étape 32).

Le porte-monnaie stocke alors la nouvelle signature électronique, en remplacement de celle correspondant à l'opération de crédit échouée, et les données caractéristiques de la nouvelle transaction, puis envoie à la banque une information d'acquittement autorisant la transaction (étape 33). Le remplacement de la première signature électronique correspondant à la transaction interrompue par la nouvelle signature électronique est réalisé au moyen du procédé de mise à jour sécurisée de mémoire EEPROM décrit dans la demande de brevet FR 95 01791.

Si le compte bancaire de l'utilisateur n'a pas été débité lors de la première transaction, la banque effectue le débit puis, dans tous les cas, elle ordonne le chargement du porte-monnaie, c'est l'étape 34.

BNSDOCID: <FR 2757661A1>

Dans l'exemple de la figure 4B, le compte bancaire a été débité avant l'interruption de la première transaction. Dans ce cas, la banque ordonne le chargement du contenu du porte-monnaie juste après avoir reçu l'information d'acquittement autorisant la transaction.

Le porte-monnaie efface la nouvelle signature de la transaction simultanément à l'opération de crédit (étape 35).

De la même manière, une transaction financière peut avoir lieu entre un porte-monnaie électronique et un fournisseur de services. Dans ce cas, le fournisseur de services, en échange d'un service à rendre, commande le débit d'une certaine valeur du contenu du porte-monnaie. Cette transaction entre porte-monnaie et fournisseur de services est représentée sur la figure 5A.

Lorsqu'un utilisateur demande un service (étape 100), le fournisseur de services élabore une preuve de la commande, c'est-à-dire une signature électronique correspondant à la transaction à effectuer.

Le porte-monnaie est ensuite débité de la valeur correspondant au service, 5 UV dans l'exemple de la figure 5A, et la signature et les données caractéristiques de la transaction sont simultanément enregistrées dans la mémoire EEPROM du porte-monnaie, c'est l'étape 200.

Le porte-monnaie émet alors des certificats de débit et les transmet au fournisseur (étape 300). Le fournisseur vérifie ces certificats, les enregistre et acquitte le paiement (étape 400). Le paiement ayant été acquitté, la signature électronique correspondant à la commande est effacée de la mémoire EEPROM du porte-monnaie électronique (étape 500).

BNSDOCID: <FR 2757661A1>

S'il y a une coupure entre les étapes 300 et 400, la présence de la signature dans la mémoire EEPROM du porte-monnaie témoigne d'une situation d'erreur possible. Cette situation d'erreur peut par exemple correspondre au fait que le paiement n'a pas été encaissé par le fournisseur alors que le contenu du porte-monnaie a été débité. Or, tant que le fournisseur n'est pas payé, il ne fournit pas le service requis correspondant. Pour obtenir le service qu'il a payé, l'utilisateur doit en conséquence présenter la preuve de la commande, c'est-à-dire la signature électronique correspondant à la transaction demandée, et éventuellement renvoyer les certificats de paiement s'ils n'ont pas été reçus par le fournisseur.

L'organigramme de la figure 5B décrit le déroulement de la procédure de réclamation permettant d'achever le paiement d'un fournisseur de services.

Dans l'exemple de cette figure 5B, le contenu du porte-monnaie a été débité de 5UV, lors de la première transaction correspondant à la figure 5A, alors que le paiement n'a pas été encaissé par le fournisseur, le contenu de la caisse étant resté égal à 500 UV. Le porte-monnaie transmet dans un premier temps au fournisseur les éléments de la réclamation, c'est-à-dire les données caractéristiques de la transaction échouée et la signature.

Dans le cas où le(s) certificat(s) a(ont) été reçu(s) par le fournisseur, ce dernier acquitte le paiement et la preuve de la transaction est effacée (étapes 340-350).

En revanche, dans le cas où le(s) certificat(s) n'a(ont) pas été reçu(s) par le fournisseur, celui-ci vérifie la validité de la réclamation, c'est-à-dire la présence de la signature électronique. Il élabore par

BNSDOCID: <FR 2757661A1>

ailleurs une nouvelle signature électronique qu'il transmet au porte-monnaie accompagnée d'une demande de paiement, c'est-à-dire d'une demande du (des) certificat(s) (étape 320).

Le porte-monnaie enregistre les données caractéristiques de la transaction dans la mémoire EEPROM ainsi que la nouvelle signature électronique en remplacement de la précédente, et il recalcule les certificats du débit échoué (étape 330).

Les certificats reçus, enregistrés et vérifiés, le fournisseur acquitte le paiement (étape 340). Enfin, le porte-monnaie efface la preuve de la transaction (étape 350).

La procédure de réclamation terminée, le contenu du porte-monnaie est débité, le fournisseur a encaissé le paiement et peut donc rendre le service correspondant requis par l'utilisateur du porte-monnaie électronique.

Les exemples qui viennent d'être décrits permettent de comprendre en quoi la gestion du stockage et de l'effacement de la signature est différent selon le type d'opération effectuée.

Ainsi, dans le cas d'un crédit, l'effacement de la signature et le crédit du contenu du porte-monnaie se font simultanément.

En revanche, dans le cas d'un débit, c'est l'enregistrement de la signature et le débit du contenu du porte-monnaie qui se font simultanément.

Selon une autre variante de réalisation, le procédé de transfert de données selon l'invention peut également être appliqué à une transaction d'unités de valeurs entre un organisme de jeux et une carte à puce par l'intermédiaire d'un réseau.

Dans ce cas les données transférées sont des unités de valeurs correspondant chacune à une somme d'argent

BNSDOCID: <FR 2757661A1>

définie au préalable. Le rechargement du contenu de la carte à puce est réalisé au moyen d'une banque interne à l'organisme de jeux. Par ailleurs, le contenu de la carte à puce est crédité ou débité selon que l'utilisateur a gagné ou perdu un jeu. Les transactions effectuées sont donc semblables aux transactions financières qui viennent d'être décrites.

Une signature électronique, destinée à prouver qu'une transaction a échoué, n'est utilisable qu'une seule fois: la signature d'une transaction échouée est remplacée par une nouvelle signature électronique de transaction de réclamation et, dans tous les cas, la signature est effacée lorsque la transaction a abouti.

BNSDOCID: <FR 2757661A1>

REVENDICATIONS

1. Procédé de transfert sécurisé de données par un réseau de communications, entre une première entité constituée par une carte à puce et une deuxième entité, caractérisé en ce qu'il consiste à élaborer au préalable une signature électronique, permettant de prouver l'initialisation du transfert, et à la stocker dans au moins une zone mémoire de la carte à puce puis, lorsque le transfert de données est terminé, à effacer cette signature.

2. Procédé selon la revendication 1, caractérisé en ce qu'il comporte une procédure de réclamation, cette procédure consistant à vérifier la présence ou l'absence de la signature électronique dans une zone mémoire de la carte à puce, afin de savoir si le transfert de données a échoué ou abouti.

3. Procédé selon la revendication 2, caractérisé en ce que, lorsque le transfert de données a été interrompu, la procédure de réclamation consiste en outre à:

- élaborer une nouvelle signature électronique,
- remplacer la signature du transfert échoué par ladite nouvelle signature,
- effectuer les étapes du transfert non encore exécutées, puis
- effacer la nouvelle signature lorsque le transfert est terminé.

4. Procédé selon l'une des revendications 1 à 3, caractérisé en ce que la signature est stockée de manière sécurisée dans une zone mémoire afin qu'elle ne

BNSDOCID: <FR 2757661A1>

soit accessible par l'extérieur ni en lecture ni en écriture.

5. Procédé selon l'une des revendications 1 à 4, caractérisé en ce que la zone mémoire de la carte à puce dans laquelle est stockée la signature est une zone de mémoire électriquement programmable de type EEPROM.

6. Procédé selon l'une des revendications 1 à 5, caractérisé en ce que la signature électronique est élaborée par la deuxième entité et effacée par l'électronique de la carte à puce.

7. Procédé selon l'une des revendications 1 à 6, caractérisé en ce que la signature électronique est élaborée au moyen d'un algorithme de cryptographie.

8. Procédé selon l'une des revendications 1 à 7, caractérisé en ce que les données transférées sont des unités de valeurs.

9 Procédé selon l'une des revendications 1 à 8, caractérisé en ce que la carte à puce est un porte-monnaie électronique.

10. Application du procédé selon l'une des revendications 1 à 9 à une transaction financière entre un organisme bancaire et un porte-monnaie électronique pour créditer le contenu de ce dernier, ou entre un fournisseur de services et un porte-monnaie électronique pour débiter le contenu de ce dernier.

BNSDOCID: <FR 2757661A1>

11. Application selon la revendication 10, caractérisé en ce que dans le cas où le contenu du porte-monnaie est crédité, l'opération de crédit et l'effacement de la signature se font simultanément.

12. Application selon la revendication 10, caractérisé en ce que dans le cas où le contenu du porte-monnaie est débité, le stockage de la signature dans une zone mémoire et l'opération de débit se font simultanément.

13. Application du procédé selon l'une des revendications 1 à 9 à une transaction d'unités de valeurs entre un organisme de jeux et une carte à puce.

BNSDOCID: <FR 2757661A1>

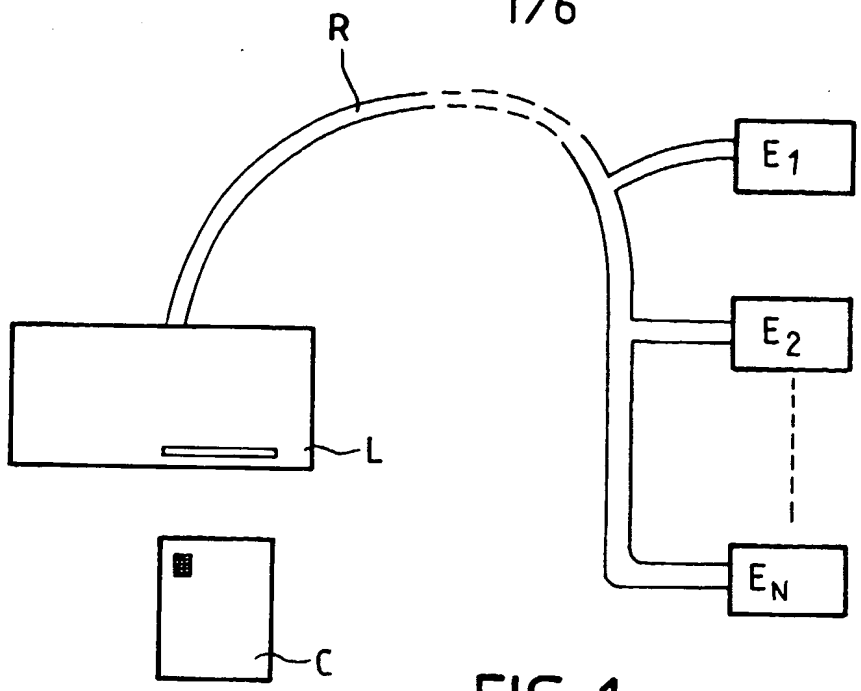


FIG_1

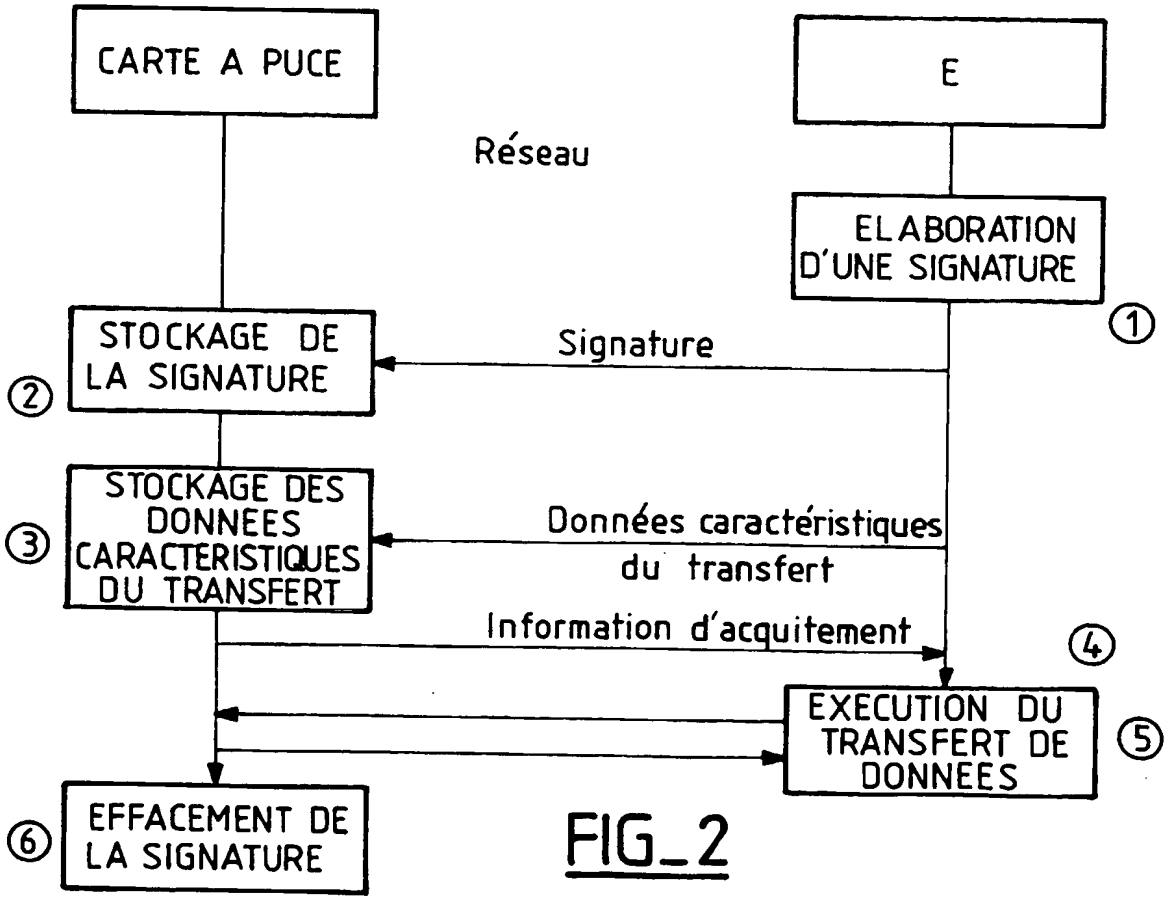


FIG_2

BNSDOCID: <FR 2757661A1>

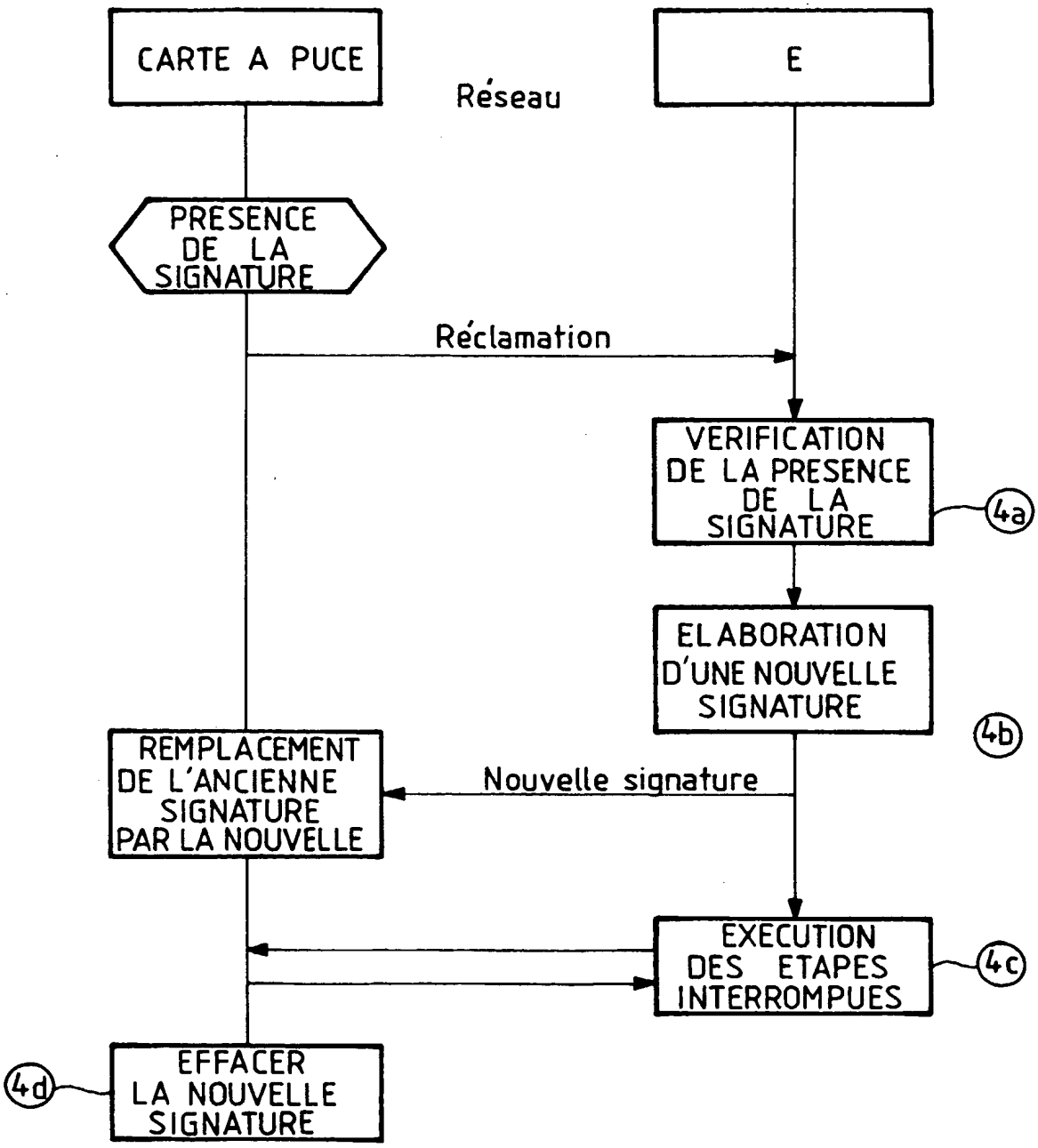


FIG_3

BNSDOCID: <FR 2757661A1>

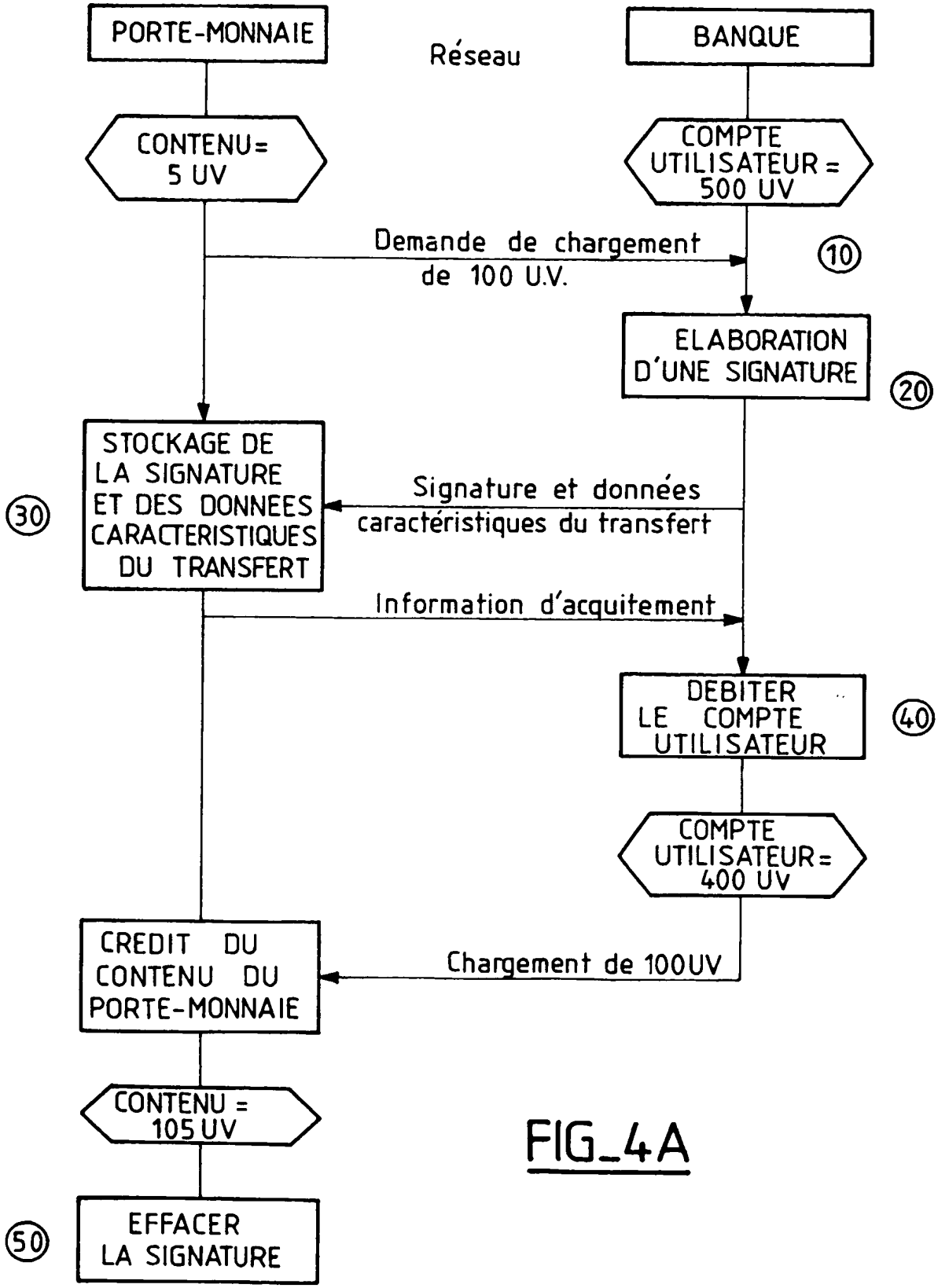


FIG_4A

BNSDOCID: <FR 2757661A1>

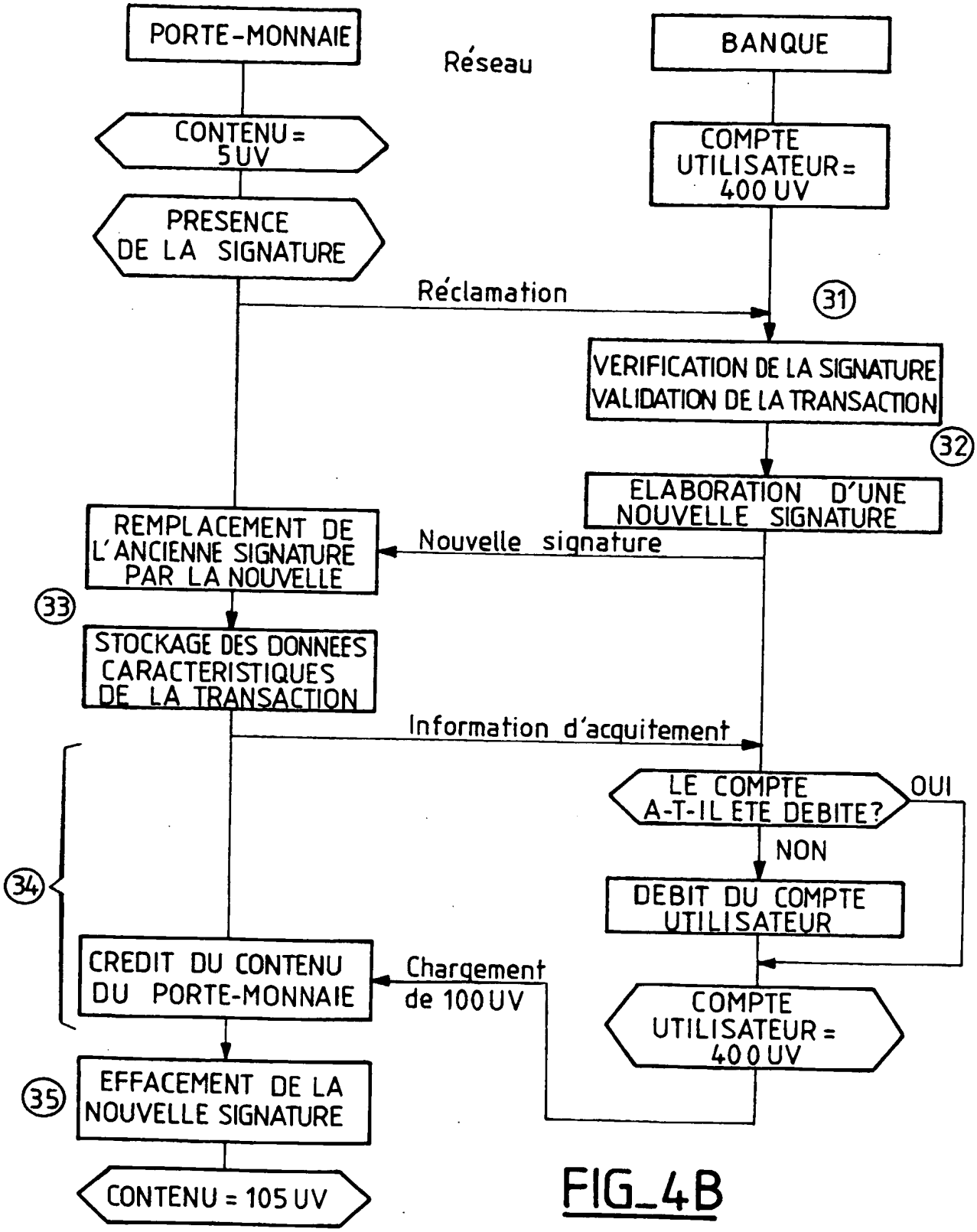


FIG_4B

BNSDOCID: <FR 2757661A1>

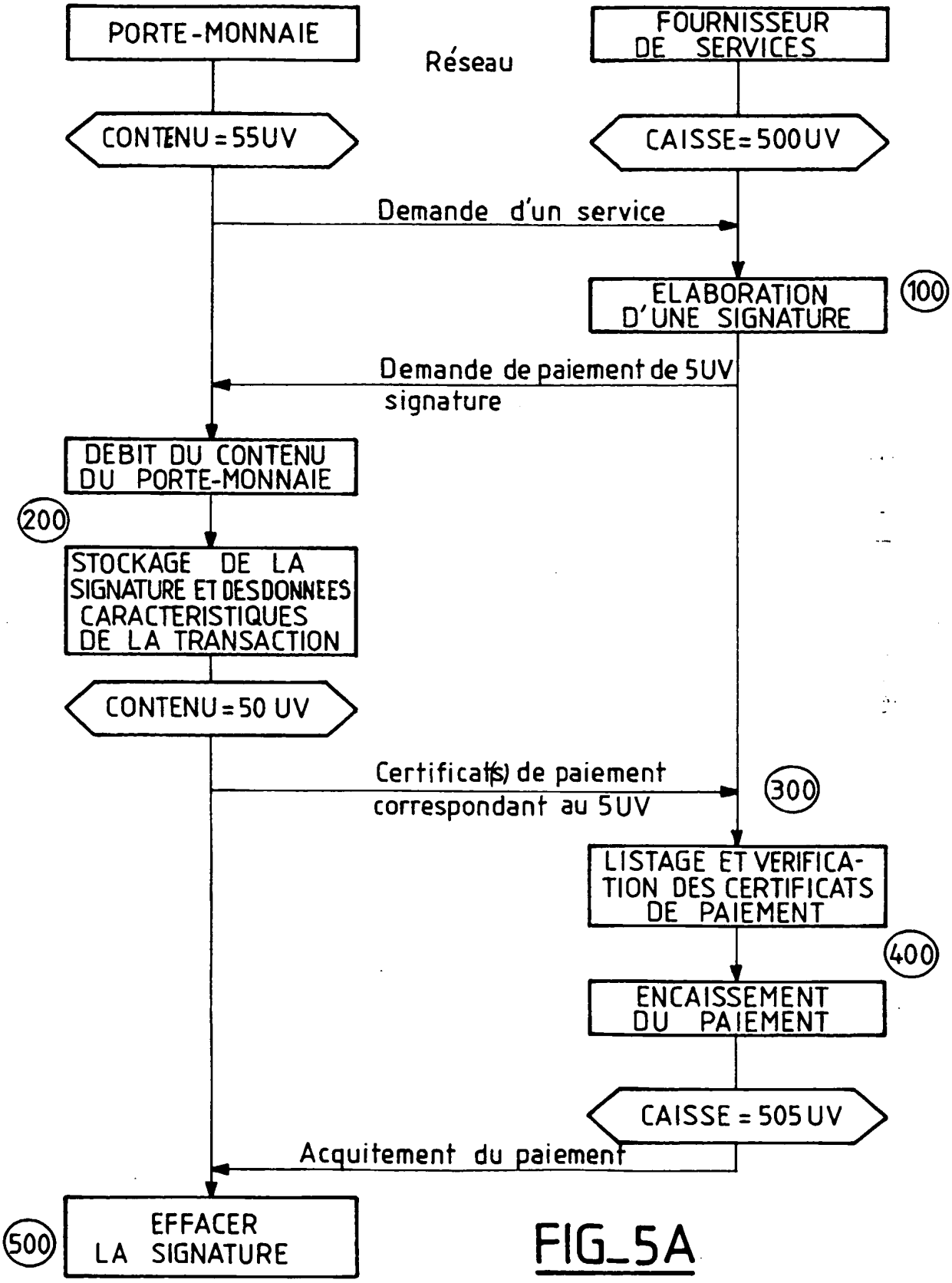


FIG_5A

BNSDOCID: <FR 2757661A1>

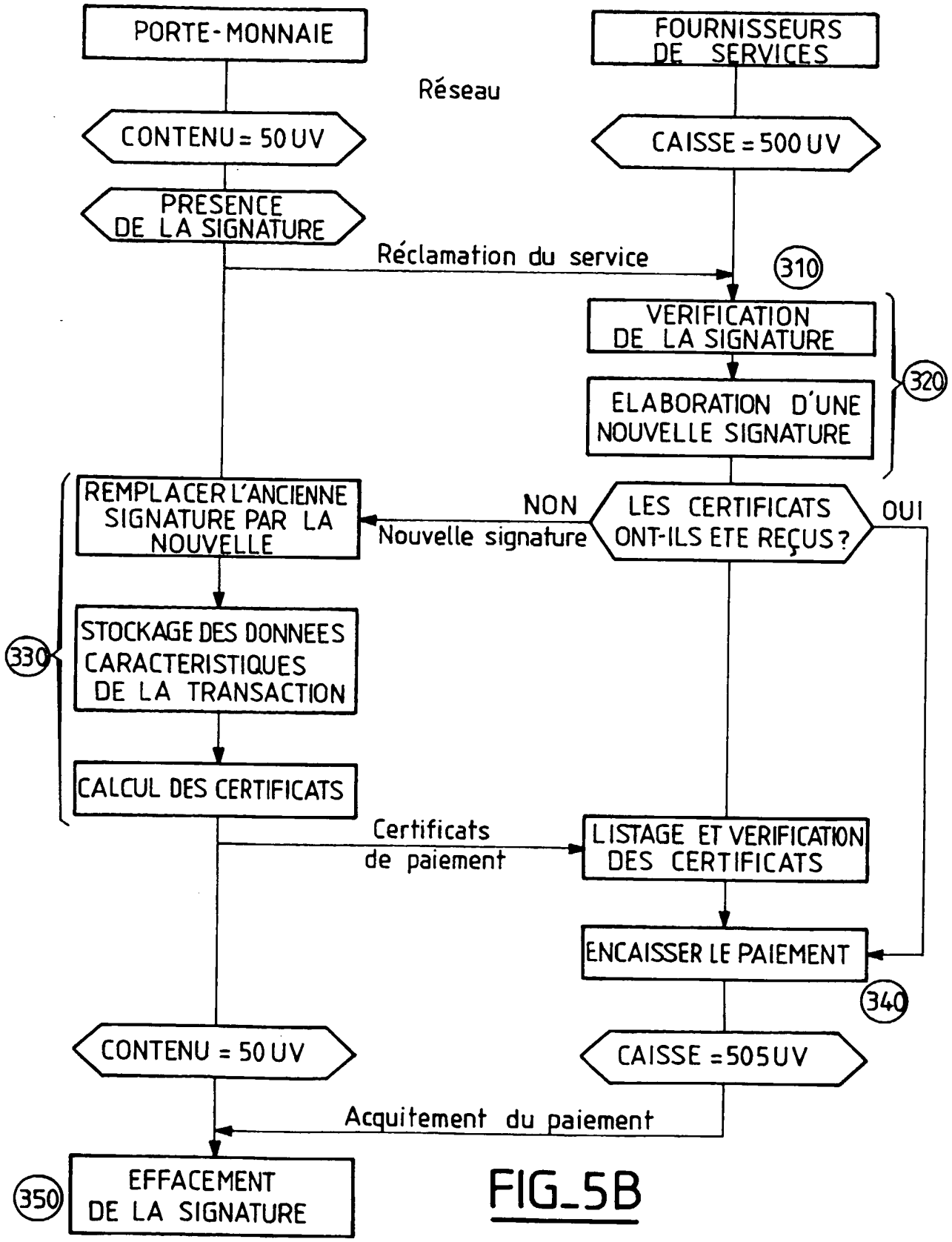


FIG_5B

BNSDOCID: <FR 2757661A1>

2757661

REPUBLIQUE FRANÇAISE

INSTITUT NATIONAL
de la
PROPRIETE INDUSTRIELLE

RAPPORT DE RECHERCHE PRELIMINAIRE

établi sur la base des dernières revendications déposées avant le commencement de la recherche

N° d'enregistrement national

FA 537485
FR 9615980

DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie	Citation du document avec indication, en cas de besoin, des parties pertinentes	Revendications concernées de la demande examinée
Y	EP 0 700 023 A (KONINKLIJKE PTT NEDERLAND) * abrégé; revendications; figures *	1,2,4,5, 8-12
Y	WO 93 08545 A (JONHIG)	1,2,4,5, 8-12
A	* abrégé; revendications; figures 3,5 * * page 11, ligne 8 - page 18, ligne 24 *	6,7
A	DE 44 39 266 A (SIEMENS)	

DOMAINES TECHNIQUES RECHERCHES (Int.CL.6)

G07F

Date d'achèvement de la recherche	Examinateur
21 octobre 1997	David, J

CATEGORIE DES DOCUMENTS CITES

X : particulièrement pertinent à lui seul
Y : particulièrement pertinent en combinaison avec un autre document de la même catégorie
A : pertinent à l'encontre d'au moins une revendication ou arrière-plan technologique général
O : divulgation non-écrite
P : document intercalaire

T : théorie ou principe à la base de l'invention
E : document de brevet bénéficiant d'une date antérieure à la date de dépôt et qui n'a été publié qu'à cette date de dépôt ou qu'à une date postérieure.
D : cité dans la demande
L : cité pour d'autres raisons

& : membre de la même famille, document correspondant

EPO FORM 1503 03.82 (P04C13)

BNSDOCID: <FR 2757661A1>

This Page Blank (uspto)